

Exhibit K

18 MAG 9 130

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION OF THE
UNITED STATES OF AMERICA FOR SEARCH
WARRANTS FOR INFORMATION AND DATA
ASSOCIATED WITH THE TWITTER ACCOUNT
@FREEJASONBOURNE; THE BUFFER ACCOUNT
WITH THE USER ID 5b8c7b5804c2e71709f92901
AND ASSOCIATED WITH THE EMAIL ADDRESS
FREEJASONBOURNE@PROTONMAIL.COM; THE
GRAVATAR PROFILE URL
HTTPS://EN.GRAVATAR.COM/JOSHSCHULTE1
(INCLUDING THE WORDPRESS SITES
JOSHSCHULTE.WORDPRESS.COM AND
PRESUMPTIONOFLAVERY.WORDPRESS.COM);
AND THE EMAIL ACCOUNTS
JOSHSCHULTE1@GMAIL.COM,
FREEJASONBOURNE@GMAIL.COM,
JOHN12GALT21@GMAIL.COM, AND
JOHNSMITH742965@OUTLOOK.COM; THE
FACEBOOK ACCOUNT WITH THE USER
IDENTIFICATION NUMBER 225303401359184;
STORED AT PREMISES CONTROLLED BY
TWITTER, INC., BUFFER, INC., AUTOMATTIC
INC., GOOGLE, INC., MICROSOFT
CORPORATION, AND FACEBOOK, INC.

SEALED
AGENT AFFIDAVIT

S1 17 Cr. 548 (PAC)

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

JEFF D. DONALDSON, being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I am a Special Agent of the Federal Bureau of Investigation (the "FBI" or the "Investigating Agency") assigned to the New York Field Office, and have been employed by the FBI since 2010. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2010 to present. In the course of my duties

JAS_021345

as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including the unauthorized retention, gathering, transmitting or losing classified documents or materials; the unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and may choose to harm the United States by misusing their access to classified information. I am also familiar, through my training and experience, with the use of computers in criminal activity and the forensic analysis of electronically stored information, including email.

2. This Affidavit is based upon, among other things, my participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals, as well as my training and experience. Because this Affidavit is being submitted for the limited purpose of obtaining the requested warrants, it does not include all the facts that I have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. In addition, unless otherwise indicated, statements by others referenced in this Affidavit were not necessarily made to me, but may have been provided to me by someone else to whom I have spoken or whose report I have read (and who in turn may have had either direct or indirect knowledge of the statement).

B. The Providers, the Target Accounts, and the Subject Offenses

3. I make this Affidavit in support of an application for search warrants pursuant to 18 U.S.C. § 2703 for all content and other information associated with the following electronic accounts:

a. The Twitter account @freejasonbourne, user identification number 1035952759252701184 (the “**Schulte Twitter Account**”), which is stored at premises controlled by Twitter Inc. (“Twitter”), headquartered at 1355 Market Street, Suite 900, San Francisco, California 94103;

b. The Buffer account with the user identification number 5b8c7b5804c2e71709f92901 and associated with the email address freejasonbourne@protonmail.com (the “**Schulte Buffer Account**”), which is stored at premises controlled by Buffer, Inc. (“Buffer”), headquartered at 44 Tehama Street, San Francisco, California 94105;

c. The Gravatar profile URL <https://en.gravatar.com/joshschulte1> (the “**Schulte WordPress Account**”), which includes the sites joshschulte.wordpress.com (the “**Schulte WordPress Site-1**”), presumptionofslavery.wordpress.com (the “**Schulte WordPress Site-2**,”), and presumptionofinnocence.net (the “**Schulte WordPress Site-3**,” and together with the **Schulte WordPress Site-1** and the **Schulte Word Press Site-2**, the “**Schulte WordPress Sites**”),¹ which are stored at premises controlled by Automattic Inc. (“Automattic”), headquartered at 60 29th Street #343, San Francisco, California 94110;

¹ Based on my review of the **Schulte Word Press Sites**, it appears that when a user tries to access the **Schulte Word Press Site-2**, the user is redirected to the **Schulte WordPress Site-3**.

d. The email accounts joshschulte1@gmail.com (the “**Schulte Gmail Account-1**”), john12galt21@gmail.com (the “**Schulte Gmail Account-2**”), and freejasonbourne@gmail.com (the “**Schulte Gmail Account-3**,” and together with the **Schulte Gmail Account-1** and the **Schulte Gmail Account-2**, the “**Schulte Gmail Accounts**”), which are maintained at premises controlled by Google, Inc. (“Google”), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The Government executed two search warrants on the **Schulte Gmail Account-1** (the “Original Gmail Search Warrants”) on or about March 14, 2017 and on or about May 17, 2017. In this application, the Government seeks a search warrant for the contents of the **Schulte Gmail Account-1** from May 18, 2017 through the present;

e. The email account Johnsmith742965@outlook.com (the “**Schulte Outlook Account**”), which is maintained at premises controlled by Microsoft Corporation (“Microsoft”), headquartered at 1 Microsoft Way, Redmond, Washington 98052; and

f. The Facebook page with the user identification number 225303401359184 and which is entitled “who is JOHN GALT?” (the “**Schulte Facebook Page**”), which is maintained at premises controlled by Facebook, Inc. (“Facebook,” and together with Twitter, Buffer, Automattic, Microsoft, and Google, the “Providers”), headquartered at 1 Hacker Way, Menlo Park, California 94025.

g. The **Schulte Twitter Account**, the **Schulte Buffer Account**, the **Schulte WordPress Account** (including the **Schulte WordPress Sites**), the **Schulte Facebook Page**, the **Schulte Outlook Account**, and the **Schulte Gmail Accounts** are collectively referred to herein as the “**Target Accounts**.”

4. The information to be searched is described in the following paragraphs and in Attachment A attached separately to each of the four proposed warrants, one to be directed to each of the Providers.

5. As detailed below, there is probable cause to believe that the **Target Accounts** contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 401 (contempt of court), 793 (unlawful disclosure of classified information), 1030 (unauthorized computer access), 1503 and 1512 (obstruction of justice), 1791 (smuggling contraband into a federal detention facility), and 2252A (illegal acts related to child pornography), as well as conspiracies and attempts to violate these provisions and aiding and abetting these offenses, among other statutes (the "Subject Offenses").

C. Services and Records of the Providers

6. Based on my training and experience, my participation in this investigation and others, my review of reports prepared by others, and my conversations with other law enforcement agents and others, I have learned the following about the Providers:

Information About Twitter

a. Twitter offers electronic messaging and online social media services. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users to post and read 280-character messages called "tweets," and to restrict their "tweets" to individuals whom they approve. In addition, Twitter's subscribers can send "direct messages," or "DMs" to other subscribers, which are typically only viewable by the sender or recipient of the direct message. These features are described in more detail below. A subscriber using Twitter's services can access his or her account from any computer connected to the Internet.

b. Twitter maintains the following records and information with respect to every subscriber account:

i. *Biographical Information:* Twitter allows its users to create personal profile pages. These pages include a short biography, photographs of the users, and location information for the user.

ii. *Tweets:* As discussed above, Twitter's users can use their accounts to post "tweets" of 280 characters or fewer. Each tweet includes a timestamp that displays when the tweet was posted. Twitter's users can also "favorite," "retweet," or reply to tweets of other users. In addition, when a tweet includes a username, often preceded by "@," Twitter designates that tweet a "mention" of the identified user. In the "Connect" tab for each account, Twitter provides the user with a list of other users who have favorite or retweeted the user's own tweets, as well as a list of all tweets that include the user's username (*i.e.*, a list of all mentions and replies for that username). By enabling the "Tweet With Location" feature, Twitter's users can also choose to include location data in their tweets.

iii. *Photographs/Images:* Twitter users can also include photographs or images in their tweets. Each account is provided a user gallery, which stores photographs or images that the user has shared on Twitter's network, including photographs or images that were uploaded from another service.

iv. *Link Information:* Twitter's users can also include links to a website in their tweets. By using Twitter's linking service, a longer website link can be converted into a shortened link, which allows it to fit into the 140-character limit. The linking service measures how many times a link has been clicked.

v. *Associated Users:* A user can also “follow” other users, which means that the user subscribes to the other users’ tweets and site updates. Each user profile page includes a list of the people who are following that user (i.e., the user’s “followers” list) and a list of people whom that user follows (i.e., the user’s “following” list). Twitter’s users can “unfollow” users whom they previously followed, and they can also adjust the privacy settings for their profile so that their tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A user can also group other users into “lists” that display on the right side of the user’s home page. Twitter also provides users with a list of “Who to Follow,” which includes recommendations of accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

vi. *Direct Messages:* A user can also send direct messages, or DMs, to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users.

vii. *Subscriber and Billing Information:* Twitter collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Twitter also maintains records concerning the date on which the account was created, the Internet protocol (“IP”) address of the user at the time of account creation, the current status of the account (e.g., active or closed), the length of service, and the types of services used by the subscriber. Additionally, for paying subscribers, Twitter maintains records of the subscriber’s means and source of payment, including any credit card or bank account number.

viii. *Search Information:* Twitter includes a search function that enables its users to search all public tweets for keywords, usernames, or subject, among other things. A user may save up to 25 past searches.

ix. *Third-Party Information:* Users can connect their accounts to third-party websites and applications, which may grant these websites and applications access to the users' public profiles with Twitter.

x. *Transactional Information:* Twitter also typically retains certain transactional information about the use of each account on its system. This information can include records of login (i.e., session) times and durations and the methods used to connect to the account (such as logging into the account through Twitter's website).

xi. *Customer Correspondence:* Twitter also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

xii. *Preserved Records:* Twitter also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

Information About Buffer

c. Buffer provides a software application that can be used through an Internet browser on a computer or a mobile device.

d. Buffer's application allows users of various social media applications to schedule their posts at various times. Buffer works with several different social media applications, including Twitter, Facebook, WordPress (an online blogging platform offered by Automattic, *see infra* ¶ 6(g)-(k), and Google+ (a social media application offered by Google, *see*

infra ¶ 6(cc)). For example, using Buffer, a user could draft a Tweet one day, but arrange for it not to publicly post on the user's Twitter page until a later date.

e. The number of posts that can be scheduled at any given time depends on the type of plan the user has purchased from Buffer. In the case of Buffer's free plan, a user can schedule up to 10 posts at once, while Buffer's "Pro" plan allows for scheduling up to 100 posts at once.

f. I believe that the information available from Buffer may include, among other things:

i. *Scheduled Social Media Posts*: Messages that were scheduled to be posted on various social media applications through Buffer's scheduling feature should be stored on Buffer's servers.

ii. *Subscriber and Billing Information*: Buffer usually collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Buffer also maintains records concerning the date on which the account was created, the IP address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services used by the subscriber. Additionally, for paying subscribers, Buffer maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iii. *Transactional Information*: Buffer also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Buffer's websites).

iv. *Cookie Data*: Buffer also typically maintains records of “cookies” used by Buffer to track information about the user of an account, including, for example, websites visited.

v. *Customer Correspondence*: Buffer also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber’s account.

Information About Automattic

g. Automattic is a web development corporation that owns and operates WordPress.com, a free-access open source online publishing and social networking website called WordPress.com, which can be accessed at <https://www.wordpress.com> (“WordPress”). WordPress allows its users to start a blog or build a website. A user can select the free basic service or pay for upgrades with advanced features such as domain hosting and extra storage. WordPress users can post content to their site, including messages, photographs, videos, and links to other websites. Some content may be geotagged. In addition, other users can comment on a blog entry that is posted on a WordPress site.

h. WordPress can be accessed through an Internet browser operating on a computer or a mobile device.

i. Automattic typically retains the following records with respect to a particular WordPress account:

i. *Subscriber Information*: Automattic retains records showing, among other things, the username, email address, name, and telephone number associated with the account.

ii. *Billing Information:* Automattic also maintains routine records related to billing.

iii. *Transactional Information:* Automattic usually retains log data, which may include the user's IP address, browser type, and operating system.

iv. *Site Creation, Posting, and Revision History Information:* Automattic maintains activity information related to the creation of a site and posting of revising information on a site. This information can include the date and time at which the site was created, the IP address used to create the site or post information to the site, and posts, including deleted posts.

v. *Comment Information:* Automattic can also retain information about comments posted about an entry on a WordPress site until those comments are deleted by the site owner.

vi. *Contact Information Associated with Domain Registration:* If a user has registered a custom domain on WordPress (meaning that the domain name for the user's site would not reflect that it is a WordPress site), Automattic may have records of the contact information for the user. For example, the **Schulte WordPress Site-3** appears as "presumptionofinnocence.net," and thus does not reflect the WordPress domain, "wordpress.com."

j. Wordpress also can provide the content of information associated with a given website or blog. In addition to the documents described above, that may include additional functionality added to the website or blog by its owner in the form of software known as widgets or plugins. It may also include a website or blog avatar or gravatar. An avatar is a picture associated with the owner of the website or blog; a gravatar is a Globally Recognized Avatar, from the website Gravatar.com or a plugin on WordPress, which differs from an avatar in that it

follows a user from website to website. When a user leaves a comment on a website or posts to a blog that supports Gravatar, the user's gravatar is pulled from Gravatar servers and appears next to the user's comment. The Gravatar.com website attempts to appear in the user's language by detecting the language settings that are configured in the user's browser. From the Gravatar.com website, a user can manage all the images and email addresses assigned to a Gravatar.com profile. Gravatar.com images can be associated with email addresses. When creating a gravatar, the Gravatar.com service asks to which registered email the image should be applied, if any.

k. Gravatar.com is another website owned and operated by Automattic and provides free gravatar profiles. Automattic includes a gravatar profile in every WordPress account.

Information About Facebook

l. Facebook owns and operates a free-access, social-networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows Internet users to establish accounts with Facebook, which they can use to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

m. Facebook asks users to provide basic contact information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, contact email addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

n. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook

users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust, to control, for example, the types of notifications they receive from Facebook.

o. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "Mini-Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

p. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

q. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's

purposes, a user's "Photoprint" includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by anyone else that have that user tagged in them.

r. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to email messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

s. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

t. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

u. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

v. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that user's access or use of that application may appear on the user's profile page.

w. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

x. Facebook also retains IP logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

y. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service used, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

z. Facebook typically maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to Section 2703(f).

Information About Microsoft and Google

aa. Microsoft and Google (together the “Email Providers”) offer email services to the public. In particular, Microsoft allows users to subscribers to maintain email accounts under, among others, the domain name “outlook.com” while Google allows subscribers to maintain email accounts under the domain name “gmail.com.” A subscriber using the Email Providers’ services can access his or her email account from any computer connected to the Internet.

bb. In addition, Google offers an online social media service. Specifically, Google allows subscribers to maintain “Google+” accounts. Through his or her Google+ account, a user can create a profile page, which contains (generally unverified) background information about the user. Among other services, a Google+ user can upload content to his or her account through posting. In addition, Google+ allows subscribers to create “circles,” which are groups of contacts that the subscriber creates and organizes. The subscriber can disseminate private content to particular circles.

cc. The information available from the Email Providers may include the following:

i. *Email Contents:* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber’s account, or stored in draft form in the account, is maintained on the Email Providers’ servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the Email Providers’ computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Email Providers’ servers for a certain period of time.

ii. *Address Book*: The Email Providers also allow subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and Billing Information*: The Email Providers collect and maintain (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. The Email Providers also maintain records concerning the date on which the account was created, the IP address of the user at the time of account creation, the current status of the account (e.g., active or closed), the length of service, and the types of services used by the subscriber. Additionally, for paying subscribers, the Email Providers maintain records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional Information*: The Email Providers also typically retain certain transactional information about the use of each account on its system. This information can include records of login (i.e., session) times and durations and the methods used to connect to the account (such as logging into the account through the Email Providers' websites).

v. *Search History*: The Email Providers also typically record searches done by a user of an account through their search engines.

vi. *Cookie Data*: The Email Providers also typically maintain records of "cookies" that they use to track information about the user of an account, including, for example, websites visited.

vii. *Customer Correspondence*: The Email Providers also typically maintain records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

viii. *Google Drive Content*: Google provides users with a certain amount of free “cloud” storage, currently 15 gigabytes, through a service called “Google Drive” (users can purchase a storage plan through Google to store additional content). Users can purchase enhanced storage capacity for an additional monthly fee. Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content “in the cloud,” *i.e.*, online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

ix. *Google Docs*: Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called “Google Docs.” Users can use Google Docs to create online documents that can be stored on or saved to the user’s Google Drive.

x. *Google Photos*: Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or “Exif”) data, and can include GPS location information for where a photo or video was taken.

xi. *Google Calendar*: Google provides users with an online calendar, in which they can add appointments, events, and reminders, that is synchronized across registered

computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

xii. *Google Chats and Google Hangouts Content:* Google allows subscribers to engage in “chat” sessions in an instant-messaging format with other Google users, the transcripts of which are generally stored in a user’s email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user’s email and chat content.

xiii. *Location History Data:* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or “apps”) or services provided by Google. For example, Google collects information collected from GPS, WiFi networks, cell site locations, and mobile networks to estimate a user’s location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device’s most recent location data in connection with a Google account.

xiv. *Google Payments:* Google allows for the storage of payment information associated with a Google account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

xv. *Google+:* Google hosts an Internet-based social network. Among other things, users can post photos and status updates and group different types of relationships (rather than simply “friends”) into Circles. In addition, Google has a service called PlusOne, in which Google recommends links and posts that may be of interest to the account, based in part on accounts in the user’s Circle having previously clicked “+1” next to the post. PlusOne information

therefore provides information about the user of a given account, based on activity by other individuals the user has entered in the user's Circle.

xvi. *Google Voice*: Google provides a telephone service that provides call forwarding and voicemail services, voice and text messaging.

xvii. *Preserved Records*: The Email Providers also maintain preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to Section 2703(f).

D. Jurisdiction and Authority to Issue the Warrant

7. Pursuant to Section 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as Google, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

8. A search warrant under Section 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

9. When the Government obtains records under Section 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. *Id.* § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. *Id.* § 2705(b).

II. Facts Establishing Probable Cause

A. Overview

10. As described in further detail below, through this application, the Government seeks a warrant related to the **Target Accounts** because they appear to be the facilities through which Joshua Adam Schulte—a former employee of the Central Intelligence Agency (“CIA”) charged with, among other things, dissemination of classified information and possession of child pornography—has conducted or intends to conduct an “information war” against the United States from the Metropolitan Correctional Center (“MCC”) by disclosing classified information and other sensitive information protected by a protective order, and by publishing false exculpatory information in an effort to defend against the crimes of which Schulte has been charged.

11. On October 3, 2018, law enforcement officers searched the MCC pursuant to a search warrant signed by the Court on October 2, 2018 (the “MCC Search Warrant”). The MCC Search Warrant and underlying affidavit are attached to this application as Exhibit A and are incorporated by reference, including the defined terms identified therein. During that search, the officers reviewed documents from Schulte’s cell (the “Schulte Cell Documents”), which showed that Schulte intended to engage in a systematic disclosure of protected information to, among others, the media.² The **Target Accounts**—which were identified through the review of the Schulte Cell Documents, as well as emails Schulte sent and received through three encrypted email accounts (“Encrypted Account-1,” “Encrypted Account-2,” “Encrypted Account-3,” and together the “Encrypted Accounts”)—are social media and email accounts that Schulte appears to intend to use (or has used) to facilitate his disclosure efforts.

² The Schulte Cell Documents were first reviewed by a wall team pursuant to a procedure set forth in another search warrant executed on October 3, 2018.

12. Thus, as described in more detail below, there is probable cause to believe that the **Target Accounts** contain evidence of the Subject Offenses, including, among other things, evidence of Schulte's unlawful dissemination to third parties (including the press) of classified information and material subject to a protective order, and evidence of Schulte's public disclosure of such protected information on publicly available Internet pages, where it could be accessed by anyone.

B. Schulte's "Information War"

13. On October 3, 2018, I and other law enforcement officers executed the MCC Search Warrant. Prior to the search, MCC officials had removed the Schulte Cell Documents, among other things, from Schulte's former cell and stored them in an official office at the MCC.

14. Based on my training and experience, my participation in this investigation and others, my conversations with other law enforcement agents and others, and my review of records provided in response to grand jury subpoenas and the Schulte Cell Documents, I have learned, among other things, the following:

a. The Schulte Cell Documents contain, among other things, documents that Schulte appeared to be preparing for public dissemination, including:

i. Various versions of "articles" or "chapters," in which Schulte wrote about his experience in prison and his views with respect to the prosecution against him. The FBI found versions of 10 of these articles (the "Schulte Articles") through other sources as well, including from members of Schulte's family to whom Schulte gave the Articles for purposes of dissemination. Some of the versions of the Schulte Articles that have been recovered (including versions Schulte sent to his cousin for public dissemination) contain classified information.

ii. Drafts of a "press release" in which Schulte accused the FBI of engaging in terrorism and declared his candidacy for Congress (the "Press Release").

iii. A document that appears to be an article for release by WikiLeaks.org (“WikiLeaks”), in which a purported FBI “whistleblower” claimed to have provided the discovery in this case to WikiLeaks and that the FBI had planted evidence of child pornography on Schulte’s computer to frame him (the “Fake FBI Document”).

iv. Drafts of a tweet (the “Fake CIA Tweet”) that appear to have been drafted around August 30, 2018,³ in which Schulte—pretending to be a former CIA colleague—claimed that two other former CIA colleagues, both of whom Schulte referred to by full name and one of whom he described as the “Peter Strzok of the CIA,” had “set up” Schulte and used him as a “scapegoat” for “Vault 7,” which is the name of WikiLeaks serial disclosures of CIA material that began on or about March 7, 2017 and which forms the basis of some of the current charges against Schulte. On the following page of the Schulte Cell Documents appears the text “Just to authenticate me first” followed by other apparent draft tweets that discussed the CIA’s alleged activities and methods, some of which appear to be classified (the “Fake Authentication Tweets”).⁴ I believe that Schulte planned to potentially publish the Fake Authentication Tweet before the Fake CIA Tweet in an effort to purportedly verify the author’s employment with the CIA and knowledge of the information in the Fake CIA Tweet.

v. Drafts of Facebook posts (the “Facebook Posts”) in which Schulte—posing as one or more of his friends—claimed that the FBI had “openly banned and burned” his writings, and that, as a result of this alleged harassment, Schulte’s Facebook page would be

³ Not all of the entries in the Schulte Cell Documents have readily apparent dates.

⁴ It is unclear from the Schulte Cell Documents whether the Fake Authentication Tweets were meant to be a single tweet with the Fake CIA Tweet or separate tweets that were to be published along with the Fake CIA Tweet.

managed by his friends going forward, rather than his family, in order to relieve “pressure” on his family.

b. The Schulte Cell Documents also show that Schulte was planning to send discovery in this case and potentially classified information to third parties, including by using encrypted email accounts and some of the **Target Accounts**. For example, Schulte wrote:

i. “If govt doesn’t pay me \$50 billion in restitution & prosecute the criminals who lied to the judge and presented this BS case then I will visit every country in the world and bear witness to the treachery . . . that is the USG [United States Government]. I will look to breakup diplomatic relationships, close embassies, and U.S. occupation around the world & finally reverse U.S. jingoism. If this one the way the U.S. govt treats one of their own, how do you think they treat allies?”

ii. “I NEED my discovery to be released to the public. I NEED my articles to be updated.”

iii. “Maybe get discovery leaked and articles updated then give all my stuff to [defense counsel] and leave for VA.”

iv. “Unable to copy over discovery to DVD. Went to law library, used laptop of Cheeno + Sardy; Laptop unable to write to DVD, drive, etc. MY laptop unable to read DVD. So, laptop that can read the DVD can’t write to it & laptop that could write to it, can’t read from it. Connect to wifi hotspot? VM?” I believe that here, Schulte is discussing his inability to use an MCC laptop to copy his discovery to a DVD, and the possibility of transferring that discovery instead by connecting one of the laptops to the Internet through a wireless network.

v. A notation that appears to indicate that Schulte intended to post the Fake CIA Tweet on the **Schulte Twitter Account**.

vi. What appears to be a “to-do” list dated September 12, 2018, in which Schulte wrote that on September 17 and 18, he would “DL Disc. UL WL,” and that on September 19, 20, and 21, he would “schedule tweets[.]” I believe that here, “DL Disc. UL WL” means that Schulte planned to download his discovery (“DL Disc.”) from the Schulte Laptop and upload that discovery to WikiLeaks (“UL WL”). As noted above, in another place in the Schulte Cell Documents, Schulte drafted the Fake FBI Document, a purported statement by a supposed FBI “whistleblower” who provided Schulte’s discovery to WikiLeaks and claimed that the FBI had planted evidence of child pornography on Schulte’s computer. *See supra* ¶ 14(a)(iii). I further believe that “schedule tweets” means that Schulte intended to schedule tweets, including the Fake CIA Tweet, using the **Schulte Buffer Account**, which, as described above, would allow him to time the disclosure of the tweets through the **Schulte Twitter Account**, *see supra* ¶ 6(c)-(f).

vii. “I thought I convinced him [Schulte’s father] to setup a protonmail email acct for me to upload the articles,” which is potentially a reference to the Schulte Articles.

viii. “Create new protonmail: presumedguilty@protonmail.com . . . migrate wordpress to protonmail.”

ix. “The way is clear. I will set up a wordpress of [the **Schulte WordPress Site-1**] and presumptionofinnocence.wordpress.com. From here, I will stage my information war: . . . The presumption of innocence blog will contain my 10 articles”⁵

x. “Yesterday I started cleansing the phone & in the process setup a new protonmail which I transferred the wordpress too [*sic*].” I believe that when Schulte wrote that he

⁵ “Presumptionofinnocence.wordpress.com” and the “presumption of innocence blog” appear to be references to **Schulte WordPress Site-3**, which at the website “presumptionofinnocence.net.”

had “started cleansing the phone,” he was referring to his efforts to delete data and/or encrypt one of the Contraband Cellphones that he used at the MCC, discussed in more detail below.

xi. “Facebook I will rename, simply ‘Who is John Galt?’ or ‘Who is Josh Schulte?’ From FB, I will post links to the articles and the blogs as I write them. The presumption of innocence blog will only contain my 10 articles 1-10, ending on the presumption of innocence. I will post each of them on the FB & delete the previous articles. From my blog, I will write about my time, etc.” Here, I believe that Schulte was referencing his plans to publish his articles, including the Schulte Articles, on the **Schulte Facebook Page**.

xii. In an entry that appears to be dated September 11, 2018, Schulte appeared to indicate that he planned to “update Facebook” (which I believe is a reference to the **Schulte Facebook Page**) by “chang[ing] password,” “delet[ing] articles,” and “chang[ing] name[.]” The entry also seemed to indicate that—as part of his updating of the **Schulte Facebook Page**—Schulte also intended to upload to the account the Facebook Posts, in which he falsely claimed that the FBI was “burn[ing]” his writings, *see supra* ¶ 14(a)(v).

xiii. An entry, which appears to be dated September 17, 2018, in which Schulte wrote, “I posted the FB thing . . . on the John Galt page & changed the pw. We’ll see what happens! Maybe a little interest? In a week I’m going to dump all my stuff.” I believe that here, Schulte is confirming that he had updated the **Schulte Facebook Page** in the manner described in Paragraph [] of this affidavit. Schulte also wrote in this entry, “My articles I’m working through with Joel. He edited articles 1&2; Hopefully I can perfect them soon. Ideally for release on the 25th but maybe not?” Here, I believe that Schulte is indicating that he hopes to publicly disseminate his articles (potentially on the **Schulte Facebook Page**) on September 25, 2018, Schulte’s birthday this year.

C. Schulte's Transfer of Data Out of the MCC

15. As described in more detail in the MCC Search Warrant, a confidential source (the "CS")⁶ has described to the FBI, in substance and in part, how, among other things, Schulte and another inmate, Omar Amanat, used cellphones smuggled into the MCC (the "Contraband Cellphones") to, among other things, communicate with people outside of the MCC and to help prepare a "report" for Amanat to submit in connection with his sentencing proceeding.⁷ See Ex. A at pp. 9-18. The CS further reported, in substance and in part, that the CS had been able to take screenshots of the Contraband Cellphones.

16. Based on my training, experience, and participation in this investigation, I know that inmate phone calls and emails at federal detention facilities, like the MCC, are recorded. Thus, inmates at times attempt to smuggle contraband electronic devices into the MCC, such as the Contraband Cellphones, in order to covertly communicate with others while in prison. In addition, many cellphones can also be used as a Wi Fi hotspot, which means that other devices can connect to the Internet through a network created by the cellphone. I also know that inmates will use such electronic devices to access email and social media accounts, like the **Target Accounts**, that will allow them to communicate discreetly, including about criminal conduct. As a result, the fact that an email account is located on a Contraband Cellphone and used to send or receive

⁶ The CS is facing immigration and narcotics trafficking charges, and is cooperating in the hope of receiving a cooperation agreement with the Government, a more lenient sentence, and potential immigration benefits. As described in this affidavit and in the MCC Search Warrant, information provided by the CS has been at least partly corroborated by, among other things, a seizure of at least one contraband cellphone and documentary evidence, including emails.

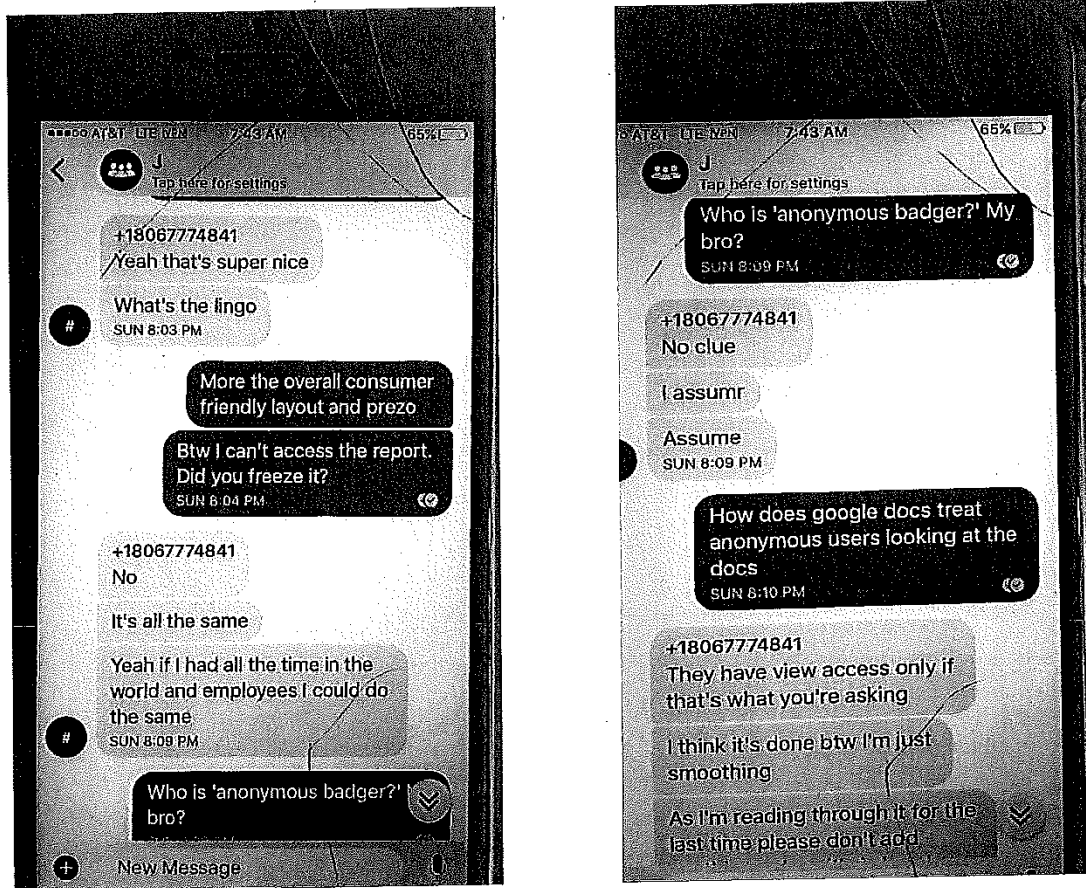
⁷ As described in more detail in the MCC Search Warrant, the "report" appears to deal with emails that Amanat fabricated and sought to introduce into evidence during his trial before the Honorable Paul G. Gardephe.

communications, on its own, demonstrates that the account likely contains communications evidencing crimes, including the Subject Offenses.

17. Based on my training and experience, my participation in this investigation, my conversations with other law enforcement agents and others, and my review of, among other things, the Schulte Cell Documents, the screenshots taken of the Contraband Cellphones by the CS, responses to grand jury subpoenas, and emails in the **Schulte Gmail Account-1** that were produced to the FBI pursuant to the Original Gmail Search Warrants and emails in the Encrypted Accounts that were reviewed pursuant to a search warrant, I have learned, among other things, that:

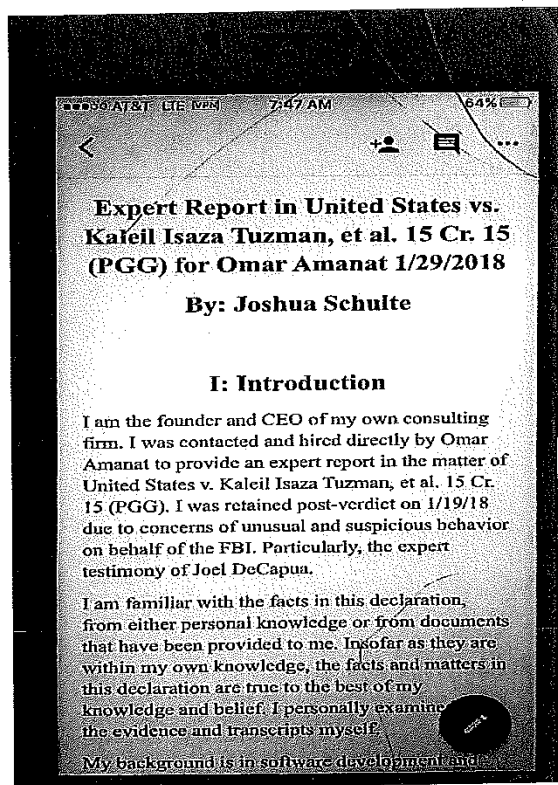
a. The CS took several screenshots of one of the Contraband Cellphones (the “Amanat Contraband Cellphone”) engaging in electronic communications with a contact identified as “J.” As discussed below, I believe the contact “J”—which is linked to a telephone number (the “806 Number”) with an 806 area code (which covers Schulte’s hometown of Lubbock, Texas, among other place)—is Schulte’s Contraband Cellphone.

b. These screenshots appear to capture a conversation concerning work by “J,” whom I believe to be Schulte, on a “report,” including:



c. In these screenshots, I believe that Schulte (“J,” texting in the gray bubbles) is instructing Amanat (texting in the blue bubbles) on how a third party could edit the “report” that was shared with them through Google Docs, a document-sharing service provided by Google.

d. One of the screenshots taken by the CS depicts what appears to be the first page of a purported “expert” report in Schulte’s name (the “Schulte Report”), which was apparently prepared in connection with Amanat’s case:



e. Both the Schulte Cell Documents and one of the Encrypted Accounts contain a handwritten document that appears to be a draft of the Schulte Report. In this draft, Schulte claimed to be an expert in a number of topics on the basis of his CIA employment. Schulte opined that an FBI expert witness called at Amanat's trial had testified falsely about emails that Amanat had sought to introduce into evidence. As described in more detail in the MCC Search Warrant, during that trial, the Government introduced evidence that Amanat had fabricated those emails. *See Ex. A at p. 9.*

f. The 806 Number is a Google Voice number, which means, as described above, that it is linked to a specific Gmail account. Subscriber information for the 806 Number indicates that it is associated with the **Schulte Gmail Account-1**.

g. Based on my review of the contents of the **Schulte Gmail Account-1** pursuant to the Original Gmail Search Warrants, I know that Google often captures communications with a Google Voice number in the Gmail account, and produces them in response to a search warrant. For example, on or about March 7, 2017, the day that WikiLeaks first made public the CIA information, the **Schulte Gmail Account-1** contained several texts between Schulte and others concerning the leak.

h. The Schulte Cell Documents also include handwritten documents (the “Location Documents”) describing potential hidden locations on hard drives or other electronic storage devices in which a user can secretly store data (“Covert Partitions”). One of the ways to identify Covert Partitions is to identify slack space on a hard drive or storage device. Slack space is the unused space between partitions on the drive. The Location Documents appear to identify the sectors where slack space is available, *i.e.*, the Covert Partitions, on a hard drive or storage device using the Windows operating system.⁸

i. Schulte also used Encrypted Account-1 to communicate with another email account (the “iCloud Account”). During one such communication in or about September 2018, Schulte requested that the individual using the iCloud Account purchase a specific electronic device (the “Device”). The Device is capable of transferring data from an electronic data storage location, such as a computer hard drive, to a cellphone, or vice versa. Based on my review of records obtained concerning the suspected user of the iCloud Account, I have learned, among other things, that the user of the iCloud Account arranged for the purchase of a piece of equipment with capabilities similar to those of the Device.

⁸ On or about October 16, 2018, the Government obtained a search warrant to search two laptops used by Schulte since his detention to determine if, among other things, he had created or used any Covert Partitions to store data. That review is ongoing.

j. On or about October 5, 2018, MCC officials recovered at least one of the Contraband Cellphones. The recovered Contraband Cellphone contained an “SD card,” which is a device that is capable of storing data for transfer from one device to another. For example, an SD card can be used to transfer data from a laptop (like the discovery laptops housed at the MCC) to a cellphone (like the Contraband Cellphones).

k. Using Encrypted Account-1, Schulte also, among other things, sent a reporter (“Reporter-1”) search warrant affidavits (the “Protected Affidavits”) designated pursuant to the protective order in this case (*see* 17 Cr. 548 (PAC), Dkt. No. 11 (the “Protective Order”)),⁹ and at least one document containing classified information.

D. Schulte Creates the Target Accounts and Tries to Hide His Use of Them

18. Based on my training and experience, my participation in this investigation and others, my conversations with other law enforcement agents and others, and my review of, among other things, subscriber information for most of the **Target Accounts**,¹⁰ I have learned, among other things, the following:

- a. The **Schulte Gmail Account-1** was created on or about April 5, 2006, and is subscribed in the name “Josh Schulte.”
- b. The **Schulte Gmail Account-2** was created on or about April 15, 2018, and is subscribed in the name “John Galt.”

⁹ On May 21, 2018, the Court held a conference at which it reminded Schulte of the terms of the Protective Order, including that Schulte could not share documents covered by the Protective Order with third parties, like reporters, who are not involved in his defense. Schulte acknowledged that he understood the terms of the Protective Order.

¹⁰ Grand jury subpoenas that call for production of the subscriber information for the **Schulte Gmail Account-3** and the **Schulte Outlook Account** are pending.

c. The **Schulte Facebook Page** was created on or about April 17, 2018, and is registered to **Schulte Gmail Account-2**.

d. The **Schulte WordPress Accounts** were created on or about August 14, 2018. The “username” of the account is “joshschulte1”; the “display name” is “Joshua Schulte”; and the email associated with the account is Encrypted Account-3.

e. The **Schulte Twitter Account** was created on or about September 1, 2018, and the email associated with the account is Encrypted Account-2. The last recorded activity in the **Schulte Twitter Account** occurred on or about October 2, 2018.

f. The **Schulte Buffer Account** was created on or about September 3, 2018, and was created by the user of Encrypted Account-2. The Schulte Buffer Account is also linked to the **Schulte Twitter Account**. The last recorded activity on the **Schulte Buffer Account** occurred on or about September 7, 2018.

19. Based on my training and experience, my participation in this investigation and others, my conversations with other law enforcement agents and others, and my review of, among other things, the Schulte Cell Documents, I have learned the following:

a. The Schulte Cell Documents include a page that appears to be dated August 21, 2018, and which seems to reflect a “to do” list for Schulte. That list includes the following items:

i. “Delete all Google Docs from johnsmith.” There is a checkmark next to this entry.

ii. “Delete all emails from johnsmith.” There is a checkmark next to this entry.

iii. “Delete suspicious emails from my gmail.” The number next to this entry is circled, and is followed by what appears to be the following four sub-items:

1. "New logins from phones[;]"
2. "Paypal[;]"
3. "WordPress[;]" and
4. "PW changes[.]"

iv. "Create new protonmail: presumedguilty@protonmail.com." This entry has a checkmark next to it.

v. "Migrate wordpress to protonmail." There is no checkmark next to this entry.

b. The following page contains what appears to be a list of, among other things, several email, social media, and encrypted messaging applications together with passwords for those accounts, including:

- i. Two of the three Encrypted Accounts;
- ii. The **Schulte Twitter Account**;
- iii. The **Schulte Gmail Account-2**;
- iv. The **Schulte Gmail Account-3**; and
- v. The **Schulte Outlook Account**.

c. Based on my examination of these two pages, and my review of, among other things, the Schulte Cell Documents and the contents of the Encrypted Accounts, I believe that Schulte was planning how to evade detection, including by destroying incriminating evidence in accounts he used (*e.g.*, "Delete suspicious emails from my gmail") and by transferring his work to a more secure, encrypted platform ("Migrate wordress to protonmail"). Furthermore, I believe that—given the location of the page and the fact that, as described in further detail below, Schulte has used these accounts to transfer protected information, *see infra* ¶¶ 21-23—the list of accounts

and passwords on the following page includes the accounts through which he potentially planned to disseminate his writings, including classified and otherwise protected information.

20. Based on my training and experience, my participation in this investigation, my conversations with other law enforcement agents and others, and my review of, among other things, the Schulte Cell Documents and the contents of the Encrypted Accounts, I have learned that emails in Encrypted Account-2 and Encrypted Account-3 appear to corroborate that Schulte was planning to use the **Target Accounts** to disseminate classified and sensitive information, including:

a. Encrypted Account-2 contained the following emails, among others:

i. On or about September 1, 2018, Twitter sent an email to Encrypted Account-2 stating that the user needed to “confirm your email account to complete your Twitter account [the **Schulte Twitter Account**].” This appears to be a standard, automatic email from Twitter as part of the process of creating a Twitter account.

ii. Later that day, an email account associated with Twitter sent an email to Encrypted Account-2 indicating that the **Schulte Twitter Account** had been accessed from an IP address associated with a server in Moldova. This appears to be an automatic email from Twitter intended to alert a user that an unauthorized user might be trying to gain access to the user’s Twitter account. A few hours later, Schulte, using Encrypted Account-2, sent an email back to Twitter claiming that he was not able to access the **Schulte Twitter Account**.

iii. On that same day—a day after the **Schulte Twitter Account** had purportedly been accessed from Moldova—an email account associated with Twitter sent two emails to Encrypted Account-2 indicating that the **Schulte Twitter Account** had been accessed from IP addresses associated with servers in France and Romania. The pattern of logins from

different countries in a short time period described in this subparagraph and subparagraph 15(c)(ii) is consistent with a user masking his or her true location and identity when accessing the Internet.¹¹

iv. Furthermore, on or about September 2, 2018, an email account associated with Buffer sent Encrypted Account-2 an email asking the user of the account to verify Encrypted Account-2. This was a standard, automatic email from Buffer indicating that a Buffer account linked to Encrypted Account-2 was either created or accessed that day. Records produced by Buffer in response to a grand jury subpoena show that the **Schulte Buffer Account** was created on or about September 3, 2018.

b. Encrypted Account-3 contained the following emails, among others:

i. On or about August 22, 2018, an email account associated with Automattic sent an email to Encrypted Account-3 stating that the email account associated with the **Schulte WordPress Site-1** had been changed from **Schulte Gmail Account-1** to Encrypted Account-3. As noted above, in the Schulte Cell Documents, Schulte wrote that he intended to “migrate” one or more of the **Schulte WordPress Accounts** to ProtonMail, the service provider for the Encrypted Accounts. *See supra* ¶ 14(b)(viii).

ii. On or about September 25, 2018, an email account associated with Automattic sent an email to Encrypted Account-3 congratulating the user of Encrypted Account-3 on his or her first post on the **Schulte WordPress Site-1**. As noted above, in the Schulte Cell Documents, Schulte wrote that he wished to begin publicly disclosing his “articles” on September 25, 2018, which is his birthday. *See supra* ¶ 14(b)(iii).

¹¹ While Schulte was released on bail, he, or someone acting on his behalf, used The Onion Router (“TOR”) to, according to Schulte’s attorney, hide Schulte’s Internet activity from the Government.

E. Schulte Begins to Disclose and Arrange to Disclose Protected Information

21. Based on my training, experience, and participation in this investigation, as well as my conversations with others, I know, among other things, in or about September 2018, Encrypted Account-1 contained, among other things, communications in or about September 2018 between Schulte—who was pretending to be a third party acting on Schulte’s behalf—and Reporter-1. In those communications, Schulte told Reporter-1 that he would give Reporter-1 “information” on several topics if Reporter-1 published stories pursuant to a timeframe dictated by Schulte. For example, Schulte stated:

a. “If you can consent to an embargo on disclosure of the information for a limited time we would give you an exclusive to the information spanning several topics.” Reporter-1 agreed to the embargo.

b. “We have decided to share with you an initial expose (depending on how the first one goes with you we will share up to 9 more) involving Russian Oligarchs business ties and wire transfers involving hundreds of millions of dollars to [a U.S. Official and the U.S. Official’s associates].”

c. As discussed above, Schulte also sent Reporter-1 the Protected Affidavits and at least one document containing classified information. *See supra* ¶ 17(k).

22. Based on my training and experience, my participation in this investigation, my conversations with other law enforcement agents and others, and my review of the Schulte Cell Documents and information publicly available about the **Target Accounts**, I have learned, among

other things, that Schulte has posted versions of parts of the Schulte Cell Documents on some of the **Target Accounts** already, including¹²:

a. On or about September 18, 2018, Schulte posted a version of the Facebook Posts, see supra ¶ 14(a)(v), on the **Schulte Facebook Account**. In this post, Schulte falsely claimed that the FBI had “burned” Schulte’s writings.

b. On or about September 25, 2018, Schulte posted a version of the Press Release on the **Schulte WordPress Site-1**. In the post, Schulte claimed, among other things, that the FBI is a terrorist organization, and declared his intention to run for Congress.

c. On or about September 25, 2018, Schulte posted another post on the **Schulte Facebook Account**. In this post, Schulte (pretending to be someone else) wrote, among other things, that:

- i. It was Schulte’s 30th birthday.
- ii. The purported writers of the post had “issued a press release on his [Schulte’s] behalf.” The purported writers then included a link to the **Schulte WordPress Site-1**.
- iii. “Josh is finally able to speak out despite the government’s attempt to silence him. He is coordinating with friends who are posting his writings in blog format.”
- iv. “What’s next? Setup of Twitter and tweets via snailmail to Twitter.”

This message was followed by an image of a cartoon face crying from laughter.

d. On or about October 1, 2018, Schulte posted an “article” that appears in the Schulte Cell Documents on the **Schulte WordPress Site-1**. On the site, the “article” is entitled “Master of Whisperers,” and in it, Schulte wrote, among other things:

¹² The posts described in this paragraph are undergoing a classification review by the CIA. It appears, however, that the versions of the posted documents described herein omit some of the classified information that was contained in other versions of these same documents.

i. “I now believe the government planted the CP after their search warrants turned up empty—not only to save their jobs and investigation, but also to target and decimate my reputation considering my involvement in significant information operations and covert action.” As noted above, in the Fake FBI Document in the Schulte Cell Documents, a purported FBI “whistleblower” claimed that the FBI had placed child pornography on Schulte’s computer after its initial searches of the device were unsuccessful in recovering evidence. *See supra* ¶ 14(a)(iii).

ii. “So who’s responsible for Vault 7? The CIA’s own version of the FBI’s Peter Strzok and Lisa Page.” As noted above, in the September Tweet in the Schulte Cell Documents, a purported former CIA colleague of Schulte (but who was in fact simply Schulte himself) claimed that two other CIA former colleagues, one of whom Schulte described as the “Peter Strzok of the CIA,” had conspired to blame Schulte for Vault 7, WikiLeaks’ disclosure of the CIA material. *See supra* ¶ 14(a)(iv).

e. On or about October 8, 2018, Schulte posted versions of nine of the Schulte Articles on the **Schulte WordPress Site-2** and the **Schulte WordPress Site-3**¹³ (the “October 8 WordPress Posts”). In one of the posted “articles,” Schulte—while stating that his statements were not intended as a “threat”—wrote

The United States government has a vital interest in safeguarding national security and especially the names of those who nsf [sic] their lives to spy on their own countries for the US. Does it seem like a good idea, then, to directly compromise and jeopardize these people? I don’t think in the history of intelligence something so idiotic has even been done, but leave it to the US to be the first to do it. Let’s take our own people worth billions of dollars of intelligence and let’s illegally throw them in prison and start fucking with them until they are bankrupt and completely compromised and vulnerable. The United States government has done the job of a foreign adversary to exploit its own intelligence

¹³ As noted above, when a user accesses the **Schulte WordPress Site-2**, the user is redirected to the **Schulte WordPress Site-3**. Thus it appears that content posted on one of the sites may also be posted on the other site. *See supra* ¶ 3(c) n.1.

officers. Essentially, it's the same as taking a soldier in the military, handing him a rifle, and then begin beating him senseless to test his loyalty and see if you end up getting shot in the foot or not. It just isn't smart.

23. Based on my training and experience, my participation in this investigation and others, my conversations with other law enforcement agents and others, and my review of, among other things, the Schulte Cell Documents and publicly available information about the Providers and the **Target Accounts**, I believe that the foregoing facts show that Schulte appears to be scheduling the posting of excerpts of the Schulte Cell Documents and/or the Schulte Articles on the **Target Accounts**, such as the Fake FBI Document and the Fake CIA Tweet, including:

a. On or about October 2, 2018, MCC officials placed Schulte into a secure housing unit (the "SHU") within the MCC, which should have restricted his access to the Contraband Cellphones.

b. Nevertheless, the October 8 Postings still appeared on the **Schulte WordPress Site-2** and the **Schulte WordPress Site-3**. As a result, it appears that Schulte arranged for the October 8 Postings either by asking another person to post them after or by using the WordPress feature that allows a user to schedule content to post at a later date himself to have the October 8 Postings posted. Either way, the timing of the October 8 Postings suggests that Schulte is scheduling the public disclosure of his writings through the **Target Accounts**.

c. The Fake CIA Tweet was drafted around August 30, 2018, days before the **Schulte Twitter Account** and the **Schulte Buffer Account** were created.

d. As described above, the Schulte Cell Documents contain a notation to "schedule Tweets" at a later date apparently on or about September 18 and September 20. *See supra* ¶ 14(b)(vi).

e. To date, Schulte does not appear to have publicly released any information through the **Schulte Twitter Account**. However, as discussed above, the **Schulte Buffer Account** allows Schulte to schedule the **Schulte Twitter Account's** future tweets.

f. Despite the fact that the **Schulte Twitter Account** does not appear to have publicly tweeted any messages between the date of its creation and October 2, 2018, the account was accessed more than 20 times, with the final login occurring on or about October 2.

g. I believe that the foregoing indicates that Schulte may have scheduled additional posts for public disclosure on the **Schulte WordPress Sites**, the **Schulte Twitter Account**, and the **Schulte Facebook Page**.

III. Evidence, Fruits and Instrumentalities in Target Accounts

24. Based on the foregoing, I respectfully submit that there is probable cause to believe that Schulte, through the use of the Contraband Cellphones and other prison contraband, has publicly disclosed material protected by the Schulte Protective Order (such as the Protected Affidavits) and classified information, and that he intends to disclose more such material. I also submit that there is probable cause to believe that Schulte was using this prison contraband to help Amanat submit a fraudulent "report" in Amanat's pending criminal proceeding. Furthermore, I submit that there is probable cause to believe that the **Target Accounts** appear to be at least some of the facilities through which Schulte has and intends to make his disclosures of protected information. Moreover, I submit that there is probable cause to believe that the **Target Accounts** will also contain evidence of potential child pornography offenses and obstruction of justice. In particular, Schulte has made certain allegations in the Schulte Cell Documents and on some of the **Target Accounts** with respect to the child pornography crimes with which he is charged, which constitute evidence of the charged offenses.

25. Based on the foregoing, I believe the **Target Accounts** are likely to contain, among other things, the following information:

- a. Evidence of the identity(ies) of the user(s) of the **Target Accounts**, the Contraband Cellphones, and the Encrypted Accounts, as well as other coconspirators in contact with the **Target Accounts**, the Contraband Cellphones, and the Encrypted Accounts;
- b. Evidence relating to the geolocation of the users of the **Target Accounts**, the Contraband Cellphones, and the Encrypted Accounts, at times relevant to the Subject Offenses;
- c. Evidence relating to the participation in the Subject Offenses by the CS, Schulte, Amanat, and others using or in communication with the **Target Accounts**, the Contraband Cellphones, and the Encrypted Accounts;
- d. Evidence concerning financial institutions and transactions used by the users of the **Target Accounts**, the Contraband Cellphones, and the Encrypted Accounts, in furtherance of the Subject Offenses;
- e. Communications evidencing crimes, including the Subject Offenses;
- f. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user(s) of the Contraband Cellphones, the Encrypted Accounts, or the **Target Accounts**; and
- g. Passwords or other information needed to access any such computers, accounts, or facilities.

26. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under Section 2703, or for the collection or production of responsive records. Accordingly, the warrants requested herein will be transmitted to the Providers, which will be directed to produce a digital copy of any responsive records to law


enforcement personnel within three days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the electronically stored information and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachments A-1 and A-2 to the requested warrants, which shall not be transmitted to the Providers.

27. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all content associated with the **Target Accounts**. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, to the extent applicable, including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

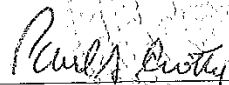
IV. Request for Non-Disclosure and Sealing Order

28. The existence and scope of this ongoing criminal investigation are not publicly known. As a result, premature public disclosure of this Affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, given that targets of the investigation are known to use computers and electronic communications in furtherance of their activity, the targets could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation. Accordingly, there is reason to believe that, were the Provider to notify the subscriber(s) or others of the existence of the requested warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of 30 days from issuance, subject to extension upon application to the Court, if necessary.

29. For similar reasons, I respectfully request that this Affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and Affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.


Special Agent Jeff D. Donaldson
Federal Bureau of Investigation

Sworn to before me this
26th day of October 2018


THE HONORABLE PAUL A. CROTTY
United States District Judge
Southern District of New York